Certificados de firmas digitales

Manual de Usuario

CAMARA DE COMERCIO DE GUAYAQUIL

SecurityDATA

Manual de usuario

Certificados de firmas digitales

CAMARA DE COMERCIO DE GUAYAQUIL

SecurityDATA

INDICE

- Terminología y definiciones..... **5**
- Servicios que le ofrece la CCG..... **9**
- El procedimiento de compra..... **9**
- Requisitos..... **12**
- Pasos para la instalación de los certificados raices..... **17**
- Administración del Certificado de Firma Electrónica y Encriptación..... **20**
- Certificados con encriptación..... **21**
- Procedimiento para envío y descarga de Certificado público de cifrado..... **23**

TERMINOLOGÍA Y DEFINICIONES

Persona Natural: Es una persona física que ejerce derechos y cumple obligaciones a título personal o en Representación de una empresa

Persona Jurídica: Es una empresa que ejerce derechos y cumple obligaciones a nombre de ésta.

Razón Social: Es el nombre y firma por los cuales es conocida una compañía de forma colectiva, comanditaria o anónima.

Institución Pública: Es el conjunto de organizaciones públicas que realizan la función administrativa y de gestión del Estado y de otros entes públicos con personalidad jurídica, ya sean de ámbito regional o local.

Certificado Electrónico: Es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Firma Electrónica: Es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.

Dispositivo Criptográfico o TOKEN: Es un medio físico de almacenamiento de Certificados que tienen niveles altos de seguridad.

Roaming: Es un perfil que se encuentra almacenado en un servidor seguro de Security Data disponibles para descargar en cualquier lugar y firmar o cifrar documentos.

Clave Pública y Privada: La criptografía asimétrica en la que se basa la PKI emplea un par de claves (podrían ser dos pares de claves), lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

Encriptación o Cifrado: Es la acción de proteger información para que no pueda ser leída con facilidad por cualquier persona.

ESP: Entrust Security Provider, Software que permite el manejo de certificados de firma electrónica y encriptación de correo y documentos.

Certificado raíz: es un tipo de certificado que es emitido por una autoridad certificadora (AC) y está firmado por la misma autoridad certificadora que lo emite. Este certificado permite a los navegadores identificarla como una AC de confianza, así cualquier clase de certificado emitido por esta AC, será reconocido por el browser, siempre y cuando el certificado raíz, se encuentre instalado en la lista de certificados raíz de confianza. Entre los campos principales de este certificado, se encuentran la llave pública de la autoridad, su periodo de validez, y el nombre la AC

Tipos de Certificados de Firma electrónica:

Certificados Persona Natural: Son certificados reconocidos de persona física que identifican al suscriptor como una persona natural pudiendo ser usado este certificados para temas tributarios, legales y personales.

Certificados Persona Jurídica: Son certificados

reconocidos de persona jurídica que identifican al suscriptor como Persona Jurídica (Empresa).

Certificados Funcionario Público: Son certificados reconocidos de persona física que identifican al suscriptor como una Institución Pública.

Certificados Funcionario de Empresa: Son certificados reconocidos de persona física que identifican al suscriptor como Corporación y al firmante como vinculado a esa corporación, ya sea como empleado, asociado, colaborador, cliente o proveedor.

Certificados Funcionario Representante Legal: Son certificados reconocidos de persona física que identifican al suscriptor como una corporación y al firmante como representante legal de dicha corporación.

Certificados SSL: Son certificados que relacionan un dominio de Internet con una persona jurídica o un comerciante registrado determinado, permitiendo establecer una conexión seguro de su servidor hacia los clientes.

Uso del Certificado de Firma electrónica:

Correo/Documento Firmado: Permite firmar digitalmente un correo electrónico o un documento digital.

Correo/Documento Firmado y Encriptado: Permite firmar digitalmente y encriptar un correo electrónico o un documento digital.

Conexión Web Segura: Son certificados que permiten al cliente autenticarse hacia algún servidor que maneje este tipo de autenticación.

Medio de Emisión de Certificados:
Forma en la cual un certificado digital es adquirido por el cliente para su uso.

Token Propio: Certificados emitidos en un dispositivo Criptográfico con Interface USB propios del cliente, siendo incluso un Token Biométrico. (se debe revisar modelos aceptados).

Token Security Data: Certificados emitidos en un dispositivo Criptográfico con Interface USB y autenticación mediante Código de Seguridad que proporciona Security Data.

Token Biométrico de SD: Certificados emitidos en un dispositivo Criptográfico con Interface USB y autenticación mediante Huella Digital que proporciona Security Data.

Software en Windows: Certificados que son descargados y guardados localmente en la Computadora en el almacén de Certificados de Windows.

Roaming incluye software: Certificados cuyo perfil está almacenado en un servidor de Security Data con sus respectivas seguridades, disponibles para descargar en cualquier lugar y firmar o encriptar documentos. Incluye Software ESP para realizar las funciones anteriormente mencionadas.

Archivos EPF incluye software: Certificados emitidos en archivo EPF disponibles para firmar o encriptar documentos. Incluye Software ESP para realizar las funciones anteriormente mencionadas.

Modelos de tokens
Epass 3003, Biopass 3000

SERVICIOS QUE LE OFRECE LA CCG

La Cámara de Comercio de Guayaquil le ofrece los siguientes servicios

1. Emisión de Certificados
2. Renovación de Certificados
3. Revocación de Certificados
4. Reemisión de Certificado
5. Desbloqueo de Token
6. Formateo de Token

EL PROCEDIMIENTO DE COMPRA

El interesado define el tipo de certificado que requiere se presenta con los requisitos que se solicitan para cada tipo de certificado en la CCG.

El ejecutivo de Cuenta de la CCG valida y confirma la documentación recibida, digitaliza la documentación y emite la liquidación para el pago del Certificado.

El interesado realiza el pago y recibe su token de ser el caso.

El interesado se dirige al balcón de servicios para que se le entregue la carpeta con las instrucciones para el registro del certificado en él se entregan todas las instrucciones para su registro, en este paso se entrega la mitad de una clave para el registro y por correo electrónico le es enviada la otra parte de la clave para completar el proceso por cuestiones de seguridad.

El formato de la documentación entregada al momento de la compra es:

1. Instalar Certificados Raíces
Descargar el certificado raíz del sitio WEB http:// www.securitydata.net.ec/descargas/ y seguir los pasos del manual para su instalación

2. Emitir el Certificado de Firma Electrónica y Encriptación

- **Certificado en Software o CAPI de Windows:**
- Mediante Internet Explorer debe ingresar a: https:// micertificado.securitydata.net.ec
- Seleccionar la Opción CREAR MI CERTIFICADO y luego CREAR CERTIFICADO EN CAPI O TOKEN.
- Ingresar los dos códigos proporcionados:
  a) Número de Referencia
  b) Código de Autorización
- Seleccionar EMITIR, una vez realizado el procedimiento se emite el certificado, el mismo que se instalará en el almacén Personal de Windows.

Certificado en Token usb o dispositivo biométrico

- Instalar JAVA en su computador
  a) Sistema Operativo de 32 bits: http://www.securitydata.net.ec/descargas/JAVAx32.rar
  b) Sistema Operativo de 64 bits: http://www.securitydata.net.ec/descargas/JAVAx64.rar
- Debe haber instalado previamente los drives del Token en su computador

- Mediante Internet Explorer debe ingresar a:
  c) TOKEN USB: https://micertificado.securitydata.net.ec
  d) Biopass3000: https://micertificado.securitydata.net.ec/BioPass3000
- Seleccionar la Opción CREAR MI CERTIFICADO y luego CREAR CERTIFICADO EN CAPI O TOKEN.
- Ingresar los dos códigos proporcionados:
  a) Número de Referencia
  b) Código de Autorización
- Activar la casilla EMITIR CERTIFICADO EN TOKEN
- Seleccionar EMITIR, una vez realizado el procedimiento se emite el certificado, el mismo que se instalará en el token.

Certificado en Roaming

- Debe instalar el software proporcionado de acuerdo a la arquitectura de su computadora.
  - SETUP ESP 32 BITS
  - SETUP ESP 64 BITS
- En la parte inferior Derecha de su computador junto al reloj aparece el siguiente ícono:
- Click Derecho en el ícono anterior y seleccionar "Enroll for Entrust Digital ID" y a continuación seleccionar "Siguiente".
  Ingresar los dos códigos para la activación, el primero que se le envió por correo y el segundo que se le proporcionó en la hoja impresa.
  - Número de Referencia: 12345678
  - Código de Autorización: XYZ-XYZ-XYZ

- Seleccionar "Siguiente" y en la próxima ventana también.
- En la ventana "Entrust Security Store Location" seleccionar la opción "In the Directory (work as a Roaming user)" y a continuación "Siguiente".
- Ingresar el nombre con el cual se Identificará para inicio de Sesión y seleccionar "Siguiente".
- Ingresar una contraseña para el inicio de sesión y seleccionar "Finalizar".
- Su certificado en Roaming está listo para usar con sus aplicaciones, para hacerlo debe iniciar sesión seleccionando la opción "Log In" en el ícono del paso 2

Certificado en Archivo EPF

- Mediante Internet Explorer debe ingresar a: https://micertificado.securitydata.net.ec
- Seleccionar la Opción "Emitir Mi Certificado Electrónico" y luego "Emitir Certificado Electrónico en archivo EPF"
- Hacer click en "Explorar" para elegir la ubicación donde irá almacenado el archivo EPF e ingresar un nombre para el archivo, por ejemplo "Luis Pérez"
- Ingresar los dos códigos proporcionados
  - Número de Referencia
  - Código de Autorización
- Ingresar una contraseña para el certificado en los campos de Contraseña y Confirmar contraseña que esté de acuerdo a las reglas de contraseña.
- Hacer click en "Emitir Certificado Electrónico"

- Una vez realizado el procedimiento se emite el certificado, el mismo que se almacenará en el computador del solicitante.
- Para utilizar este archivo Debe instalar el software proporcionado de acuerdo a la arquitectura de su computadora.
  - SETUP ESP 32 BITS
  - SETUP ESP 64 BITS

  NOTA: Los códigos de activación tienen una validez de 14 días. Pasado este tiempo favor comunicarse con 1800-firmas o soporte@securitydata.net.ec

La contraseña inicial para administrar su certificado es:

REQUISITOS

Los documentos solicitados se deberán enviar por e-mail escaneados A COLOR EN FORMATO PDF y con los debidos nombres (ej. Formulario.pdf, nombramiento.pdf, cedula.pdf, etc). OTRO TIPO DE FORMATO NO SERA ACEPTADO AL IGUAL QUE LOS DOCUMENTOS ESCANEADOS EN BLANCO Y NEGRO SERAN DEVUELTOS.

Requisitos Representante Legal:

A. Original de la Cédula de ciudadanía o pasaporte en casos de extranjeros.
B. Original de la Papeleta de votación actualizada, (para militares la libreta militar).
C. Original o copia certificada (notariada) del Registro único de contribuyentes (RUC) de la empresa.
D. Original o copia certificada (notariada) del Registro único de proveedores (RUP) en caso de disponerlo.
E. Original o copia certificada y legible del nombramiento del representante legal adjuntando copia clara de la cédula de ciudadanía del mismo.
F. Original del Certificado de Cumplimiento de Obligaciones emitido por la Superintendencia de Compañías u Original o copia certificada (notariada) de constitución de la Empresa solicitante.
G. Formulario de solicitud lleno y firmado.
H. Presentarse en Entidad que le proporcionó la cita físicamente para firmar el contrato, validar la identidad y emisión del certificado.

Requisitos Miembro de Empresa:

A. Original de la Cédula de ciudadanía o pasaporte en casos de extranjeros.

B. Original de la Papeleta de votación actualizada, (para militares la libreta militar).
C. Original o copia certificada (notariada) y legible del certificado laboral que certifique el cargo de la persona, actualizado, firmado por el representante legal o emitida por el departamento de recursos humanos de la entidad solicitante.
D. Original o copia certificada (notariada) del Registro único de contribuyentes (RUC) de la empresa.
E. Original o copia certificada (notariada) del Registro único de proveedores (RUP) en caso de disponerlo.
F. Original o copia certificada (notariada) y legible del nombramiento del representante legal adjuntando copia clara de la cédula de ciudadanía del mismo.
G. Original del Certificado de Cumplimiento de Obligaciones emitido por la Superintendencia de Companias u Original o copia certificada (notariada) de constitución de la Empresa solicitante.
H. Original de la Autorización firmada por el representante legal, donde conste el número, nombre y cargo de todos los solicitantes de la Empresa para emisión de certificado de Firma Electrónica.
I. Formulario de solicitud lleno y firmado.
J. Presentarse en Entidad que le proporcionó la cita físicamente para firmar el contrato, validar la identidad y emisión del certificado.

Requisitos Persona Natural:

A. Original de la Cédula de ciudadanía o pasaporte en casos de extranjeros.
B. Original de la Papeleta de votación actualizada, (para militares la libreta militar).
C. Original de la planilla de un servicio básico, que certifique

la dirección que conste en el RUC (luz, agua, teléfono, celular, Tvcable, gas o internet) de cualquiera de los últimos tres meses, a nombre de la persona que solicita el certificado. – (Si la planilla no está a su nombre o no es de la dirección del RUC NO se podrá tramitar la solicitud). Se puede aceptar también el contrato de arrendamiento del local o vivienda en el cual conste la dirección del RUC y que este a nombre de la persona que solicita el certificado. El contrato debe tener los sellos del juzgado del inquilinato + las tres últimas facturas del pago hecho

D. Original o copia certificada (notariada) del Registro único de contribuyentes (RUC) en caso de disponerlo. (Para agentes de aduana es obligatorio presentar el RUC).

E. Original o copia certificada (notariada) del Registro único de proveedores (RUP) en caso de disponerlo.

F. Ser persona física y mayor de edad.

G. Formulario de solicitud lleno y firmado.

H. Presentarse en Entidad que le proporcionó la cita físicamente para firmar el contrato, validar la identidad y emisión del certificado.

Requisitos Funcionario Público:

A. Original de la Cédula de ciudadanía o pasaporte en casos de extranjeros.

B. Original de la Papeleta de votación actualizada, (para militares la libreta militar).

C. Original o copia certificada (notariada) y legible del nombramiento o "Acción de Personal" del solicitante o a su vez un certificado laboral que certifique el cargo del funcionario público, actualizado, firmado por el representante legal o emitida por el departamento de recursos humanos de la institución.

D. Original o copia certificada (notariada) del Registro único de contribuyentes (RUC) de la institución

E. Original o copia certificada (notariada) del Registro único de proveedores (RUP) en caso de disponerlo.
F. Original o copia certificada (notariada) y legible del nombramiento del representante legal adjuntando copia clara de la cédula de ciudadanía del mismo.
G. Original o copia certificada (notariada) y legible del Registro Oficial donde conste la creación de la Institución.
H. Autorización firmada por el representante legal, donde conste el número de solicitudes, nombre y cargo de todos los solicitantes de la Empresa para emisión de certificado de Firma Electrónica.
I. Formulario de solicitud lleno y firmado.
J. Presentarse en Entidad que le proporcionó la cita físicamente para firmar el contrato, validar la identidad y emisión del certificado.

PASOS PARA LA INSTALACIÓN DE LOS CERTIFICADOS RAICES

1. Descargar los certificados raíces del sitio WEB y proceda a almacenarlos en su máquina (No cambie los nombre de los archivos).

a) Certificado CA Raíz: https://www.securitydata.net.ec/descargas/windows/cacert.cer

b) Certificado CA Subordinada: https://www.securitydata.net.ec/descargas/windows/subcert.cer

2. Instalación en el Sistema Operativo **Windows**

a. Certificado CA Raíz

i. Click en el certificado cacert.cer

ii. Seleccionar Instalar Certificado

iii. Se ejecuta el Wizard o Ayudante de Importación y dar click en Siguiente.

iv. Seleccionar la Opción: Colocar todos los

certificados en el siguiente almacén y seleccionar examinar

v. Seleccionar la opción Entidades de Certificación Raíz de Confianza, y dar click en Aceptar.

vi. Seleccionar Siguiente,

vii. Seleccionar Almacén de Certificados seleccionados por el usuario y dar click en Finalizar

viii. El sistema Pregunta si ¿Desea Instalar el certificado? Seleccionar Si

ix. Aparece un mensaje de certificado Instalado correctamente y damos click en Aceptar.

b. Certificado CA Subordinada

i. Click en el certificado subcert.cer

ii. Seleccionar Instalar Certificado

iii. Se ejecuta el Wizard o Ayudante de Importación y dar click en Siguiente.

iv. Seleccionar la Opción: Colocar todos los certificados en el siguiente almacén y seleccionar examinar

v. Seleccionar la opción Entidades de Certificación Intermedias, y dar click en Aceptar.

vi. Seleccionar Siguiente,

vii. Seleccionar Almacén de Certificados seleccionados por el usuario y dar click en Finalizar

viii. El sistema Pregunta si ¿Desea Instalar el certificado? Seleccionar Si

ix. Aparece un mensaje de certificado Instalado correctamente y damos click en Aceptar.

3. Instalación en el Sistema Operativo de **MAC**

a. Certificado CA Raíz

i. Click en el certificado cacert.crt y se abre la aplicación de "Acceso a llaveros"

ii. Seleccionar el llavero del sistema SISTEMA y hacer click en ok

iii. El certificado ha sido instalado, se puede comprobar la instalación del certificado dando click

en Sistema del lado izquierdo de la aplicación de llaveros.

iv. Luego seleccionar Certiticados en la parte de CATEGORÍA

v. El certificado debe ser cargardo en este almacén. Se lo puedo hacer mediante arrastre del archivo cacert.crt al mismo.

vi. La aplicación le solicitará su contraseña de administrador del sistema.

vii. Ahora si aparece el certificado.

b. Certificado CA Subordinada

i. Click en el certificado subcert.crt

ii. Continuar con el mismo procedimiento del literal "ii" de la opción "Certificado CA Raíz" del paso 2 "Instalación en el Sistema Operativo de MAC".

4. Instalación **Certificado Raíz Mozilla Firefox**

a. Abrir el Navegador Mozilla Firefox

b. Ir al sitio web https://www.securitydata.net.ec/descargas/firefox/cacert.crt

c. A continuación se despliega una ventana en la cual indica ¿Quiere confiar en "AUTORIDAD DE CERTIFICACION"?, en la cual se debe activar las 3 opciones siguientes: Confiar en esta CA para identificar Sitios WEB, Usuarios de Correo, Desarrolladores de Software, y dar click en Aceptar.

d. Nuevamente seleccionar Aceptar y listo.

5. Instalación **Certificado Raíz ADOBE**

Descargar los certificados raíces del sitio WEB y proceda a almacenarlos en su máquina (No cambie los nombre de los archivos).

• Certificado CA Raíz: https://www.securitydata.net.ec/descargas/adobe/RAIZCERT.fdf

• Certificado CA Subordinada: https://www.securitydata.net.ec/descargas/adobe/SUBCERT.fdf

a. Certificado CA Raíz en FDF

i. Click en el certificado RAIZCERT.fdf

ii. Se visualiza una ventana que indica "Archivo de intercambio de datos – Importar contacto"

iii. Dar click en "Definir confianza de contactos…"

iv. En la ventana que se visualiza en la pestaña Confianza activar las casillas "Utilizar este certificado como raíz de confianza" y "Documentos Certificados" y a continuación seleccionar Aceptar.

v. Se ha instalado el certificado Raíz en Adobe.

b. Certificado CA Subordinada en FDF

i. Click en el certificado SUBCERT.fdf

ii. Continuar con el mismo procedimiento del literal "ii" de la opción "Certificado CA Raíz en FDF" del paso 4 "Instalación Certificado Raíz ADOBE".

ADMINISTRACIÓN DEL CERTIFICADO DE FIRMA ELECTRÓNICA Y ENCRIPTACIÓN

Para administrar su certificado ingrese a **https://micertificado.securitydata.net.ec**

1. Dé click en **"Administrar mi cuenta"**
2. Ingrese los datos requeridos en los campos:
   - Nombre
   - Apellido
   - Número de serie (opcional)
   - Dirección de correo electrónico que proporcionó al adquirir el certificado
3. Luego hacer click en **"Siguiente"**
4. Ingresar la contraseña proporcionada en este documento y hacer click en **"Siguiente"**
5. Ahora debe cambiar la contraseña por una elegida por usted y hacer click en **"Enviar"**

6. Si las contraseñas coinciden se la actualiza exitosamente y puede ingresar a administrar su cuenta.
7. En la parte de administración puede cambiar su contraseña, revocar el certificado, suspender el certificado o resetear la contraseña de su certificado en software o Roaming (solamente certificados de firma y encriptación).

CERTIFICADOS CON ENCRIPTACIÓN

Para el caso de aquellos clientes que adquieran certificados con encriptación el procedimiento es para firmar y cifrar documentos es el siguiente:

Firmar Documentos.

1. Conectar el Dispositivo Criptográfico si su certificado está almacenado en un Token o normal o un Token Biométrico, en caso de usar certificados en Roaming iniciar sesión a través del software ESP.
2. Click derecho en el documento y seleccionar **"Digitally Sing File".**
3. Se muestra un Wizard del software, Seleccionar **siguiente**.
4. Verificar y Seleccionar el certificado que va a usar y a continuación **Siguiente.**
5. Seleccionar Finalizar y el documento está listo.
6. Para verificar la firma Click derecho en el documento firmado y seleccionar **"Propiedades"** y en la pestaña **"Security Status"** se verifica la firma.

Encriptar Documentos.

1. Las personas que utilicen certificados de firmar y encriptación deben instalar el software ESP que les proporciona.

2. Conectar los dispositivos TOKENS o iniciar sesión en caso de usar el servicio de Roaming.
3. Seleccionar el archivo que necesita cifrar y se da click derecho y seleccionar **"Encrypt File"**
4. Se muestra un Wizard del software, Seleccionar siguiente.
5. Dar click en **"Choose"** y ubicar su certificado en el cual van a existir dos con el mismo nombre, para verificar cual es el certificado público dar doble click en cada uno de ellos y en la pestaña Detalles ubicar el campo **"USO DE LA CLAVE"** ó **"KEY USAGE",** en el cual debe indicar cifrado de clave.
6. Para cifrar para otra persona activar la casilla **"Encrypt the files for other people in addition to myself"** y dar click en siguiente.
7. Seleccionar la opción **ADD** y escribir el nombre de la persona a quien quiero cifrar.
8. Seleccionar el certificado de **CIFRADO** como se detalle en el literal **"e"**, y a continuación seleccionar OK.
9. Seleccionar Finalizar y el documento está listo.
10. Para verificar la firma y cifrado Click derecho en el documento firmado y seleccionar **"Propiedades"** y en la pestaña **"Security Status"** se verifica la firma y el cifrado.

Firmar y Encriptar.

1. Las personas que utilicen certificados de firmar y encriptación deben instalar el software ESP que les proporciona.
2. Conectar los dispositivos TOKENS o iniciar sesión en caso de usar el servicio de Roaming.
3. Seleccionar el archivo que necesita cifrar y se da click derecho y seleccionar **"Encrypt and Digitally Sign File".**
4. Para la sección de Encriptación seguir los pasos desde el literal **"e"** de la opción **"2"**.

5. Para la sección de Firmado seguir los pasos desde el literal **"d"** de la opción **"a".**

PROCEDIMIENTO PARA ENVÍO Y DESCARGA DE CERTIFICADO PÚBLICO DE CIFRADO

Envío a través del correo.

1. Conectar el Dispositivo Criptográfico si su certificado está almacenado en un Token o normal o un Token Biométrico, en caso de usar certificados en Roaming iniciar sesión a través del software ESP.
2. Ir a menú **INICIO** y seleccionar la opción **EJECUTAR** para Windows XP y para Windows Vista o 7 escribir **"certmgr.msc"** y a continuación **ENTER.**
3. Se despliega la herramienta del Almacén de Certificados, ubicar en ella la carpeta **"Personal"** y dentro de ella **"Certificados",** dar doble click en esta última.
4. Ubicar su certificado en el cual van a existir dos con el mismo nombre, para verificar cual es el certificado público dar doble click en cada uno de ellos y en la pestaña Detalles ubicar el campo **"USO DE LA CLAVE"** ó **"KEY USAGE",** en el cual debe indicar cifrado de clave.
5. En la pestaña **DETALLES** dar click en **"COPIAR EN ARCHIVO",** se ejecuta una Ayuda, seleccionamos siguiente y aparece una ventana activada la casilla **"No exportar la clave privada"** y a continuación siguiente.
6. Seleccionar la opción **"Estándar de Sintaxis de cifrado de mensajes: Certificados PKCS#7 (.P7B)"** y a continuación seleccionar **"Siguiente".**
7. Colocar el nombre al certificado y ubicar la dirección donde desea almacenar. Y seleccionar **"siguiente".**

8. Y en la ventana que aparece también **"siguiente".**
9. Listo su certificado público está exportado y puede enviarlo por correo a la persona que desea cifrar para usted.

Obtención a través del software ESP.

1. Las personas que utilicen certificados de firmar y encriptación deben instalar el software ESP que les proporciona.
2. Conectar los dispositivos TOKENS o iniciar sesión en caso de usar el servicio de Roaming.
3. Seleccionar el archivo que necesita cifrar y se da click derecho y seleccionar **"Encrypt File"**
4. Se muestra un Wizard del software, Seleccionar **siguiente.**
5. Dar click en **"Choose"** y seleccionar nuestro certificado de cifrado como se detalle en el literal **"d"** de la opción **"1".**
6. Para cifrar para otra persona activar la casilla **"Encrypt the files for other people in addition to myself".** Y dar click en siguiente.
7. Seleccionar la opción ADD y escribir el nombre de la persona a quien quiero cifrar.
8. Seleccionar el certificado de CIFRADO como se detalle en el literal **"d"** de la opción **"1",** y a continuación seleccionar OK.

Descarga desde la página web.

- Seguir los pasos del manual "Manual de Usuario-Bajar llave pública"

  http://www.securitydata.net.ec/descargas/Manual%20de%20Usuario-%20Bajar%20llave%20publica.pdf

CAMARA
DE COMERCIO
DE GUAYAQUIL

SecurityDATA

Mayor información:
1800 - FIRMAS
www.securitydata.net.ec